

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takeshi SAITO, et al.

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HEREWITH

FOR: AV DATA TRANSMISSION AND RECEPTION SCHEME FOR REALIZING COPYRIGHT PROTECTION

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- Full benefit of the filing date of U.S. Application Serial Number \_\_\_\_\_, filed \_\_\_\_\_, is claimed pursuant to the provisions of 35 U.S.C. §120.
- Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):  
Application No. \_\_\_\_\_ Date Filed \_\_\_\_\_
- Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

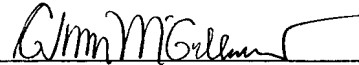
| <u>COUNTRY</u> | <u>APPLICATION NUMBER</u> | <u>MONTH/DAY/YEAR</u> |
|----------------|---------------------------|-----------------------|
| Japan          | 2003-058927               | March 5, 2003         |
| Japan          | 2003-173985               | June 18, 2003         |

Certified copies of the corresponding Convention Application(s)

- are submitted herewith
- will be submitted prior to payment of the Final Fee
- were filed in prior application Serial No. \_\_\_\_\_ filed \_\_\_\_\_
- were submitted to the International Bureau in PCT Application Number \_\_\_\_\_  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- (A) Application Serial No.(s) were filed in prior application Serial No. \_\_\_\_\_ filed \_\_\_\_\_; and
- (B) Application Serial No.(s)
  - are submitted herewith
  - will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

C. Irvin McClelland  
Registration Number 21,124

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月 5日  
Date of Application:

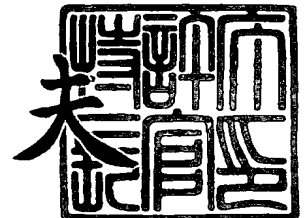
出願番号 特願2003-058927  
Application Number:  
[ST. 10/C]: [JP2003-058927]

出願人 株式会社東芝  
Applicant(s):

2003年 7月18日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康



【書類名】 特許願

【整理番号】 14153101

【提出日】 平成15年 3月 5日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 1/00

【発明の名称】 通信装置、送信装置、受信装置及び通信方法

【請求項の数】 10

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝  
研究開発センター内

【氏名】 斉 藤 健

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝  
研究開発センター内

【氏名】 磯 崎 宏

【特許出願人】

【識別番号】 000003078

【住所又は居所】 東京都港区芝浦一丁目1番1号

【氏名又は名称】 株式会社 東 芝

【代理人】

【識別番号】 100075812

【弁理士】

【氏名又は名称】 吉 武 賢 次

【選任した代理人】

【識別番号】 100088889

【弁理士】

【氏名又は名称】 橋 谷 英 俊

## 【選任した代理人】

【識別番号】 100082991

【弁理士】

【氏名又は名称】 佐 藤 泰 和

## 【選任した代理人】

【識別番号】 100096921

【弁理士】

【氏名又は名称】 吉 元 弘

## 【選任した代理人】

【識別番号】 100103263

【弁理士】

【氏名又は名称】 川 崎 康

## 【手数料の表示】

【予納台帳番号】 087654

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信装置、送信装置、受信装置及び通信方法

【特許請求の範囲】

【請求項 1】

著作権保護を図る必要のあるAVデータを暗号化、または復号化し、著作権保護のために使用される特定のプロトコルに関する情報と、ペイロードタイプの値を含むAV転送プロトコルヘッダと、を付加したAVパケットの送信または受信を行うAVデータ処理手段と、

著作権保護を施すAVデータを特定するための前記ペイロードタイプの値のネゴシエーションを、著作権保護のための認証・鍵交換処理の中で行う認証・鍵交換手段と、を備えることを特徴とする通信装置。

【請求項 2】

前記ペイロードタイプの値は、2種類以上の値、あるいは所定の範囲内の任意の値であることを特徴とする請求項 1 に記載の通信装置。

【請求項 3】

前記AVデータ処理手段によりAVデータの送信または受信を行った後に、前記認証・鍵交換手段により認証・鍵交換処理を行うことを特徴とする請求項 1 または 2 に記載の通信装置。

【請求項 4】

前記AVデータ処理手段は、前記認証・鍵交換手段により認証・鍵交換処理を行った結果、認証・鍵交換に成功した場合に、前記ペイロードタイプの値に対応するAVデータの送信または受信を行うことを特徴とする請求項 1 または 2 に記載の通信装置。

【請求項 5】

前記AVデータ処理手段がAVデータの送信または受信を行った後、該AVストリームが著作権保護を図る必要があることを報知する情報を送信または受信する著作権保護報知手段を備えることを特徴とする請求項 1 ～ 3 のいずれかに記載の通信装置。

【請求項 6】

受信装置からのAVデータの送信要求に応じて、著作権保護を図る必要のあるAVデータを暗号化し、著作権保護のために使用される特定のプロトコルに関する情報と、ペイロードタイプの値を含むAV転送プロトコルヘッダと、を付加したAVパケットを生成して送信するAVデータ処理手段と、

前記受信装置からの認証・鍵交換要求に応じて、著作権保護を施すAVデータを特定するための前記ペイロードタイプの値のネゴシエーションを、著作権保護のための認証・鍵交換処理の中で行う認証・鍵交換手段と、を備えることを特徴とする送信装置。

#### 【請求項7】

受信装置からの認証・鍵交換要求に応じて、著作権保護を施すAVデータを特定するためのペイロードタイプの値のネゴシエーションを、著作権保護のための認証・鍵交換処理の中で行う認証・鍵交換手段と、

認証・鍵交換に成功した前記受信装置からのAVデータの送信要求に応じて、著作権保護を図る必要のあるAVデータを暗号化して、前記特定のプロトコルに関する情報と、前記ネゴシエーションで受信装置の間で合意されたペイロードタイプの値を含むAV転送プロトコルヘッダと、を付加したAVデータを生成して送信するAVデータ処理手段と、を備えることを特徴とする送信装置。

#### 【請求項8】

暗号化された、著作権保護を図る必要のあるAVデータに、著作権保護のために使用される特定のプロトコルに関する情報と、ペイロードタイプの値を含むAV転送プロトコルヘッダと、が付加されたAVパケットを受信するAVデータ処理手段と、

著作権保護を施すAVデータを特定するためのペイロードタイプの値のネゴシエーションを、前記AVデータを送信した送信装置との間で著作権保護のための認証・鍵交換処理の中で行う認証・鍵交換手段と、を備えることを特徴とする受信装置。

#### 【請求項9】

暗号化された、著作権保護を図る必要のあるAVデータに、著作権保護のために使用される特定のプロトコルに関する情報と、著作権保護を施すAVデータを特

定するためのペイロードタイプの値のネゴシエーションを、送信装置との間での認証・鍵交換処理の中で行う認証・鍵交換手段と、

認証・鍵交換に成功した前記送信装置で生成された、著作権保護を図る必要のある暗号化されたAVデータに、著作権保護のために使用される特定のプロトコルに関する情報と、前記ネゴシエーションの結果、送信装置との間で合意されたペイロードタイプの値を含むAV転送プロトコルヘッダと、が付加されたAVデータを受信するAVデータ処理手段と、を備えることを特徴とする受信装置。

#### 【請求項10】

著作権保護を図る必要のあるAVデータを暗号化、又は復号化し、著作権保護のために使用される特定のプロトコルに関する情報と、ペイロードタイプの値を含むAV転送プロトコルヘッダと、を付加したAVパケットの送信または受信を行い、

著作権保護を施すAVデータを特定するための前記ペイロードタイプの値のネゴシエーションを、著作権保護のための認証・鍵交換処理の中で行うことを特徴とする通信方法。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、著作権保護を図る必要のあるAVデータを送信または受信する通信装置、送信装置、受信装置及び通信方法に関する。

##### 【0002】

#### 【従来の技術】

デジタル情報家電と呼ばれる商品が増加している。これら商品は、デジタル放送の開始などに伴い、普及が期待される商品群であり、デジタル放送対応テレビや、セットトップボックス、デジタルVTR、DVDプレーヤ、ハードディスクレコーダ等のデジタルデータ・デジタルコンテンツを扱う商品が広く含まれる。

##### 【0003】

この際、考慮すべきは著作権保護である。デジタルデータは、コピー時の品質劣化が無いなどの利点がある反面、容易に不正コピーを行えるなどの欠点も持つ

。このため、デジタルAV機器同士をつなぐデジタルネットワークであるIEEE1394には、認証・鍵交換機構や、データの暗号化の機能が兼ね備えられている（非特許文献1参照）。

#### 【0004】

さて、近年、IEEE1394に加えて、家庭内でパーソナルコンピュータ（以下、PC）を用いたネットワーク（イーサネット（登録商標）や無線LAN等）を手軽に構築できるようになった。これは、PCの普及、ブロードバンド環境の低価格化、ネットワーク対応の機器やソフトウェアの普及など、複数の理由が考えられよう。この流れに、AV機器も加わる可能性がある。

#### 【0005】

このような環境で利用されるプロトコルは、主にIP（インターネットプロトコル）である。

#### 【0006】

##### 【非特許文献1】

<http://www.dtcp.com>

#### 【0007】

##### 【発明が解決しようとする課題】

しかしながら、インターネットプロトコル自体は著作権保護を特に考慮に入れていないため、AVデータの著作権保護が十分に図れないおそれがある。特に、最近のように、無線LANやBluetooth等の無線ネットワークが普及している状況では、著作権保護の必要なAVデータが無断で複製や再生される可能性が高くなる。

#### 【0008】

本発明は、このような点に鑑みてなされたものであり、その目的は、著作権保護を図りつつAVデータの送信または受信を行える通信装置、送信装置、受信装置及び通信方法を提供することにある。

#### 【0009】

##### 【課題を解決するための手段】

上述した課題を解決するために、本発明は、著作権保護を図る必要のあるAVデータを暗号化、または復号化し、著作権保護のために使用される特定のプロトコ



ルに関する情報と、ペイロードタイプの値を含むAV転送プロトコルヘッダと、を付加したAVパケットの送信または受信を行うAVデータ処理手段と、著作権保護を施すAVデータを特定するための前記ペイロードタイプの値のネゴシエーションを、著作権保護のための認証・鍵交換処理の中で行う認証・鍵交換手段と、を備える。

#### 【0010】

##### 【発明の実施の形態】

以下、本発明に係る通信装置、送信装置、受信装置及び通信方法について、図面を参照しながら具体的に説明する。本発明に係る通信装置は、著作権保護を必要とするAVデータを送信する送信装置、及び著作権保護を必要とするAVデータを受信する受信装置の少なくとも一方を指す。

#### 【0011】

##### (第1の実施形態)

図1は本発明に係る通信装置の一実施形態である送信装置と受信装置とを備えたAV通信システムの概略構成を示すブロック図である。図1のAV通信システムは、ある家庭内のホームネットワーク1と、このホームネットワーク1に接続されている送信装置2及び受信装置3とを備えている。ホームネットワーク1の一例として、以下では無線ネットワーク1について説明するが、無線ネットワーク1の代わりに、あるいは無線ネットワーク1と並行して、イーサネットやIEEE1394等の有線ネットワークを用いてもよい。無線ネットワーク1の具体的な形態は特に問わないが、例えば、IEEE802.11a、IEEE802.11bまたはIEEE802.11gなどの各種の無線LANが考えられる。

#### 【0012】

送信装置2と受信装置3は、AVデータのやり取りを行う。送信装置2は、セットトップボックスやDVDプレーヤ等のAVデータのソースデバイスとなりうる機器である。受信装置3は、テレビ、表示装置、スピーカ、AV録画・録音装置などのAVデータのシンクデバイスとなりうる機器である。

#### 【0013】

図2は送信装置2の内部構成の一例を示すブロック図である。図2の送信装置

2は、インタフェース部11と、AVデータ生成／蓄積部12と、RTP処理部13と、著作権保護暗号化部14と、TCP/IPパケット送受信部15と、イーサネットフレーム送受信部16と、著作権保護認証・鍵交換部17とを有する。

#### 【0014】

インタフェース部11は、無線ネットワーク1に接続される部分であり、無線ネットワーク1に対してAVデータ等を送信する。AVデータ生成／蓄積部12は、受信装置3に送信するためのAVデータの生成や蓄積を行う。RTP処理部13は、タイムスタンプ処理やシーケンス番号処理などのAVデータのトランスポートレイヤ層の処理と、再生や停止などのAV制御とを行う。イーサネットフレーム送受信部16は、AVデータを含むイーサネットフレームを生成して送信するとともに、無線ネットワーク1を介して受信したイーサネットフレームを受信する。著作権保護認証・鍵交換部17は、著作権保護のために、受信装置3との間で認証や鍵交換処理を行う。

#### 【0015】

図3は受信装置3の内部構成の一例を示すブロック図である。図3の受信装置3は、インタフェース部21と、イーサネットフレーム送受信部22と、TCP/IPパケット送受信部23と、著作権保護復号化部24と、RTP処理部25と、AVデータ再生／蓄積部26と、著作権保護認証・鍵交換部27とを有する。

#### 【0016】

イーサネットフレーム送受信部22は、インタフェース部21にて受信された受信パケットからイーサネットフレームを抽出する。TCP/IPパケット送受信部23は、イーサネットフレーム送受信部22で受信されたイーサネットフレームからTCP/IPパケットを抽出する。著作権保護復号化部24は、著作権保護のために暗号化されて転送されてきたAVデータを復号化する。RTP処理部25及び著作権保護認証・鍵交換部27はそれぞれ、RTP処理部13と著作権保護認証・鍵交換部17と同様の処理を行う。

#### 【0017】

著作権保護認証・鍵交換部27が行う認証・鍵交換処理の少なくとも一部は、IPパケットを用いてなされてもよいし、IPパケットを用いずに、認証・鍵交換プ

ロトコルを直接イーサネットフレーム上に載せて行ってもよい。

#### 【0018】

本実施形態の送信装置2と受信装置3でやり取りされるデータフォーマットは図4のようなものである。データ本体を表すペイロードd1にTCP/IPヘッダd2を付加したTCP/IPパケットに、イーサネットヘッダd3を付加してイーサネットフレームが生成される。すなわち、TCP/IPパケットは、イーサネットフレームにカプセル化される。なお、TCP (Transmission Control Protocol) の代わりに、UDP (User Datagram Protocol) を用いてもよい。ホームネットワーク1が無線ネットワーク1の場合には、イーサネットフレームにさらに無線レイヤヘッダを付加して無線レイヤフレームが生成され、この無線レイヤフレームが送信装置2から送信される。

#### 【0019】

なお、図4では、簡略化のために、トレイラの存在を無視している。無線レイヤヘッダには、無線ネットワーク1上でのみ使用される制御データ、例えばIEEE 802.11無線LANにおけるFCフィールドやDur/IDフィールドなどが含まれる。

#### 【0020】

本実施形態では、著作権保護を図る必要のあるAVデータを暗号化して送信する。暗号化するのは、図4のTCP/IPパケットの部分である。この部分のより詳細なデータフォーマットは図5のようなものである。AVデータを暗号化したペイロードd5に、IETFにて標準化されたAVデータ転送用の転送プロトコルであるリアルタイム・トランスポートプロトコル (以下、RTP) ヘッダd6と、UDPヘッダd7と、IPヘッダd8を付加し、さらに、RTPヘッダd6とペイロードd5との間に、著作権保護用制御データd9を付加する。この著作権保護用制御データd9は、コピー制御情報 (以下、CCI) や、AVデータに対して施される暗号化の鍵の値の変化のタイミングを通知するための0/Eビットなどからなる。なお、著作権保護用制御データd9は、RTPヘッダの中に含めてもよい。

#### 【0021】

また、本実施形態では、RTPヘッダのペイロードタイプの値を、RTSPにて使用されるダイナミック・ペイロードタイプの値 (#z) を用いる。ここで、ダイナ

ミック・ペイロードタイプの値を用いるとは、符号化方式ごとに予め定められている割り当て済みのペイロードタイプの値を用いるのではなく、通信ごとに事前にネゴシエーションを行い、利用するペイロードタイプの値を動的に（ダイナミックに）ネゴシエーションした上で決定することを意味する。

#### 【0022】

これは、従来のRTPと異なり、ペイロードが暗号化されているため、従来のRTPフォーマットとは異なるデータがペイロードに入るという事情と、RTPヘッダとペイロードの間に著作権保護用制御データ d 9が入るという事情による。

#### 【0023】

図6は送信装置2と受信装置3が行うAVデータの暗号化伝送処理の第1の実施形態の処理手順を示すシーケンス図である。以下、この図に基づいて、第1の実施形態の暗号化伝送処理を詳しく説明する。なお、著作権保護の仕組みとして、例えば、DTCP (Digital Transmission Content Protection) を想定する。なお、DTCPの詳細については、<http://www.dtcp.com>を参照されたい。

#### 【0024】

まず、受信装置3は、送信装置2に対してAVデータの送信を要求する（ステップS1）。ここでは、IETFが規定したWebサーバのAVストリーミング機能の遠隔制御用のプロトコルであるRTSP (Real Time Streaming Protocol : RFC2326参照) を用いて、TCP/IP上にてコマンド（プロトコル）のやり取りを行う。なお、RTSP以外に、IEEE1394におけるAV/Cや、UPnP（ユニバーサル・プラグアンドプレイ）プロトコル等によっても、同様の制御を行うことができる。

#### 【0025】

RTSPでは、(1)AVストリーミング伝送に用いられる符号化方式と、そのビットレート等の各種の属性やパラメータ、(2)使用されるトランスポートプロトコル（TP）の種別（本実施形態の場合はRTP）、(3)RTPで用いられるペイロードタイプの値（本実施形態の場合、ダイナミックペイロードタイプの値を用いる）、(4)通信を行うTCP、またはUDPポート番号の値（本実施形態の場合はTCPを用いる。もちろん、実際にはUDPを用いても良い）、(5)ストリーミングの動作の規定（再生、巻き戻し、停止等）等についてのネゴシエーションを行う。

## 【0026】

上記(1)～(5)等で、送信装置2と受信装置3間で合意が得られると、送信装置2は、AVデータを暗号化した後(ステップS2)、上記RTSPで合意されたコネクション(本実施形態では、送信装置2のIPアドレス=a、送信ポート番号=#x、受信装置3のIPアドレス=b、受信ポート番号=#y)にて、転送プロトコル=RTP、合意されたダイナミックペイロードタイプ(PT)の値(=#z)にて、暗号化されたAVデータを含むAVストリームの送信を開始する(ステップS3)。

## 【0027】

ステップS3で送信されるAVストリームは図5のようなデータフォーマットである。このAVストリームを受信した受信装置3が、例えばAVストリーム中の著作権保護用制御データd9により、受信したAVデータに暗号がかけられていることを発見したとする。この場合、受信装置3は送信装置2に対して認証・鍵交換手順を要求し(ステップS4)、認証・鍵交換処理を行う(ステップS5)。認証・鍵交換処理に成功すると、受信装置3は、暗号鍵を入手する(ステップS6)。

## 【0028】

この認証・鍵交換の要求と認証・鍵交換処理は、TCP/IPパケット上で行ってもよいし、無線レイヤフレームやイーサネットフレーム上に、認証・鍵交換用のデータを直接載せて行ってもよい。また、この認証・鍵交換手順は、ホームネットワーク1内に留まるべきものであるため、TCP/IPパケット上で行う場合には、TTL(タイム・トゥ・ライブ)の値を「1」にした状態で通信を行う等の制限を設けるのが望ましい。

## 【0029】

認証・鍵交換は、特定のRTPストリームで転送されるAVストリームに関して行われる。このため、認証・鍵交換を行う前提として、「どのAVストリームに関する認証・鍵交換なのか」についてのネゴシエーションを行う必要がある場合がある。

## 【0030】

例えば、受信装置3が、受信したAVストリームが暗号化されていることを認識

し、「このAVストリームについての認証・鍵交換をさせて欲しい」と送信装置2に問い合わせる場合がある。また、送信装置2が、「このAVストリームは、暗号化して受信装置3に対して送付する。このことを、予め、あるいは、AVストリーム転送と同時に、受信装置3に対して通知し、認証・鍵交換のトリガをかけさせる必要がある」と判断し、受信装置3に対して、「このAVストリームは暗号化して送信する。よって、このAVストリームについて認証・鍵交換手順を送信装置2に対して行うべし」という通知を行う場合も考えられる。

#### 【0031】

もちろん、AVストリーム毎に個々に認証・鍵交換を行うのではなく、「送信装置2と受信装置3の間でやり取りされる、全てのRTPストリームに関して有効とするための認証・鍵交換」を最初に行い、その後は、同送信装置2と受信装置3の間でやり取りされる全てのRTPストリームに関して、上述した認証・鍵交換手順で定められた条件に従って、AVデータの暗号化を行ってもよい。

#### 【0032】

あるいは、特定のペイロードタイプの値については著作権保護を施すことを、送信装置2と受信装置3の間で予め合意しておき、このようなペイロードタイプの値をもつRTPストリームが受信された場合には、著作権保護が施されているものとしても良い（もちろん、RTSP内にて、設定しているRTPコネクションにDTCP著作権保護が施されていることをネゴシエーションする方法も考えられる）。

#### 【0033】

上述した図6は受信装置3が送信装置2に対して認証・鍵交換のトリガをかける場合の処理手順を示している。受信装置3は、何らかの方法で、受信したAVストリームが暗号化されていることを認識する。例えば、「受信したAVストリームを復号しても、所望のAVストリームを再生できない場合」、あるいは「受信したAVストリームに、図5のような著作権保護用制御データd9が付属しており、これを検出して、そのAVストリームが暗号化されていることを認識する場合」、「RTPのペイロードの値としてダイナミックペイロード用の値が用いられており、この値が、データが暗号化されている場合に使われる値であることを認識している場合」等が考えられる。

**【0034】**

受信したAVストリームが暗号化されていること、あるいはその可能性があることを認識した受信装置3は、認証・鍵交換要求を送信装置2に対して送出する。この手順もDTCPの手順の一部とすることが可能である。この場合、受信装置3は、その認証・鍵交換要求（あるいは、後続の認証・鍵交換手順パケット）にて、「どのAVストリームについての認証・鍵交換であるか」を明示する。本実施形態では、転送プロトコル種別（RTP）とRTPパケットのペイロードタイプの値（#z）の値を使う。

**【0035】**

ちなみに、送信装置2のIPアドレスとポート番号、及び受信装置3のIPアドレスとポート番号を、その認証・鍵交換要求に明記してもよいし、RTPのSSRCフィールドの値（AVソース毎に一意につけられる識別番号。詳細は、RTPのスペックであるRFC1889を参照のこと）、あるいはIPv6パケット等に含まれる「フローID」の値を用いても良い。

**【0036】**

これを受信した送信装置2は、その認証・鍵交換要求（あるいは、認証・鍵交換手続き）が、どのペイロードタイプの値のAVストリームのためのものであるかを認識した上で、認証・鍵交換手順を継続する。

**【0037】**

認証・鍵交換手順が終了すると、受信装置3は、その認証・鍵交換結果をもとに、その暗号化AVストリームの復号鍵を入手（あるいは、入手するための計算のための初期情報を取得）することができる（ステップS6）。

**【0038】**

このように、第1の実施形態では、著作権保護の必要なAVデータを暗号化したペイロードに、プロトコル種別（例えばRTP）と、このプロトコルが使用するペイロードタイプの値と、を付加したAVストリームを送信装置2から受信装置3に送信するため、このAVストリームを受信した受信装置3は、AVデータが暗号化されていることを容易に検出でき、かつ認証・鍵交換が必要なデータを容易に識別できる。これにより、著作権保護を図りつつ、AVデータを簡易かつ迅速に受信及

び再生できる。

**【0039】**

(第2の実施形態)

第2の実施形態は、AVデータを暗号化して送信したことを送信装置2から受信装置3に通知するものである。

**【0040】**

第2の実施形態の送信装置2及び受信装置3はそれぞれ図2及び図3と同様に構成されているが、AVデータの暗号化伝送処理の一部が第1の実施形態と異なっている。

**【0041】**

図7は送信装置2と受信装置3が行うAVデータの暗号化伝送処理の第2の実施形態の処理手順を示すシーケンス図である。第2の実施形態では、送信装置2が受信装置3に暗号化されたAVデータを含むAVストリームを送信した後に(ステップS13)、AVデータが暗号化されていることを通知するためのAVストリーム暗号化通知を送信装置2が受信装置3に送信する(ステップS14)。この通知は、送信装置2が送信したAVストリーム(ペイロードタイプ=#z)がDTCP等のプロトコルに従って暗号化され、これを受信装置3が復号するには、送信装置2との間で認証・鍵交換を行う必要があることを受信装置3に知らせるものである。この通知は、IPパケットを用いて行ってもよいし、無線レイヤパケット、もしくはイーサネットフレームを用いて行ってもよい。

**【0042】**

受信したAVストリーム(ペイロードタイプ#zのAVストリーム)が暗号化されることを認識した受信装置3は、認証・鍵交換要求を送信装置2に対して送出する(ステップS15)。後は、図5の場合と同様である。

**【0043】**

なお、図7では、ペイロードタイプの値として特定の値(#z)を通知する形の例を示したが、著作権保護を施すペイロードタイプの2種類以上の値からなる範囲(例えば#z1～#z2の範囲の値)を通知してもよい。

**【0044】**



このように、第2の実施形態では、AVストリーム中のAVデータが暗号化されていることを送信装置2が受信装置3に通知するため、受信装置3は、受信したAVストリーム中のAVデータが暗号化されているか否かを自分自身で調べる必要がなくなる。したがって、受信装置3の処理を軽減できるとともに、認証・鍵交換処理が完了するまでの時間を短縮できる。

#### 【0045】

(第3の実施形態)

第3の実施形態は、AVデータを送信する前に、著作権保護のための認証・鍵交換を行うものである。

#### 【0046】

第3の実施形態の送信装置2及び受信装置3はそれぞれ図2及び図3と同様に構成されているが、AVデータの暗号化伝送処理の一部が第1及び第2の実施形態と異なっている。

#### 【0047】

図8は送信装置2と受信装置3が行うAVデータの暗号化伝送処理の第3の実施形態の処理手順を示すシーケンス図である。まず、受信装置3は、送信装置2に対して、IPパケットまたはイーサネットフレームにて、認証・鍵交換を要求する(ステップS21)。そして、送信装置2と受信装置3との間で、認証・鍵交換処理を行い(ステップS22)、認証・鍵交換処理に成功すると、受信装置3は復号鍵を取得する(ステップS23)。

#### 【0048】

この認証・鍵交換の間に、「RTPのペイロードタイプの値が#z1～#z2の間の場合には、そのRTPコネクションのデータはDTCPにて著作権保護のための暗号化が施されており、更にRTPヘッダとRTPペイロードの間にDTCP用の制御データが挿入される」ということを、認証・鍵交換の段階で送信装置2と受信装置3の間で共有する。

#### 【0049】

その後、受信装置3は、送信装置2に対してAVデータの送信を要求し(ステップS24)、これを受けて送信装置2はAVデータを暗号化し(ステップS25)

、図4のフォーマットのIPパケットまたはイーサネットフレームを受信装置3に向けて送信する(ステップS26)。図8の例では、ペイロードタイプの値の範囲を#z1~#z2にして、暗号化したAVデータを伝送している。

#### 【0050】

受信装置3は、ペイロードタイプの値を参照することで、そのAVストリームがDTCPにて暗号化されていることを認識でき、適切な復号化手順を経て、AVストリームの再生を行うことができる。

#### 【0051】

この他にも、認証・鍵交換手順に、対象とするペイロードタイプの値を含めておき、そのコマンドが要求する何らかの手順(例えば、最新の鍵の値を問い合わせる等)の対象が、特定のペイロードタイプのAVストリームについてのものであることを通知する手順を加えてもよい。

#### 【0052】

このように、第3の実施形態では、受信装置3から認証・鍵交換要求を行って、認証・鍵交換処理に成功した場合に限り、送信装置2から受信装置3に対して、暗号化したAVデータを含むAVストリームを送信するため、無駄にAVストリームを送信しなくて済み、通信効率の向上が図れるとともに、セキュリティ性も向上する。

#### 【0053】

上述した図6~図8の処理は、ハードウェアで実現してもよいし、ソフトウェアで実現してもよい。ソフトウェアで実現する場合には、図6~図8の処理の少なくとも一部を実現するプログラムをフロッピーディスクやCD-ROM等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

#### 【0054】

また、図6~図8の処理の少なくとも一部の機能を実現するプログラムを、インターネット等の通信回線(無線通信も含む)を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネ

ット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

### 【0055】

#### 【発明の効果】

以上詳細に説明したように、本発明によれば、著作権保護を図る必要のあるAVデータを暗号化、または復号化し、著作権保護のために使用される特定のプロトコルに関する情報と、ペイロードタイプの値を含むAV転送プロトコルヘッダと、を付加したAVパケットの送信または受信を行うAVデータ処理手段と、著作権保護を施すAVデータを特定するための前記ペイロードタイプの値のネゴシエーションを、著作権保護のための認証・鍵交換処理の中で行う認証・鍵交換手段と、を備えることにより、送信側の装置と受信側の装置の間で、著作権保護を施すAVデータの識別を、前記ペイロードタイプの値を、そのAVデータが持っているかどうかで識別でき、もって、著作権保護を図りつつ、AVデータを簡易かつ迅速に送信・受信・再生できる。

#### 【図面の簡単な説明】

##### 【図1】

本発明に係る通信装置の一実施形態である送信装置と受信装置とを備えたAV通信システムの概略構成を示すブロック図。

##### 【図2】

送信装置の内部構成の一例を示すブロック図。

##### 【図3】

受信装置の内部構成の一例を示すブロック図。

##### 【図4】

送信装置と受信装置でやり取りされるデータフォーマットを示す図。

##### 【図5】

暗号化されたAVデータの詳細データフォーマットを示す図。

##### 【図6】

送信装置と受信装置が行うAVデータの暗号化伝送処理の第1の実施形態の処理手順を示すシーケンス図。

**【図 7】**

送信装置と受信装置が行うAVデータの暗号化伝送処理の第2の実施形態の処理手順を示すシーケンス図。

**【図 8】**

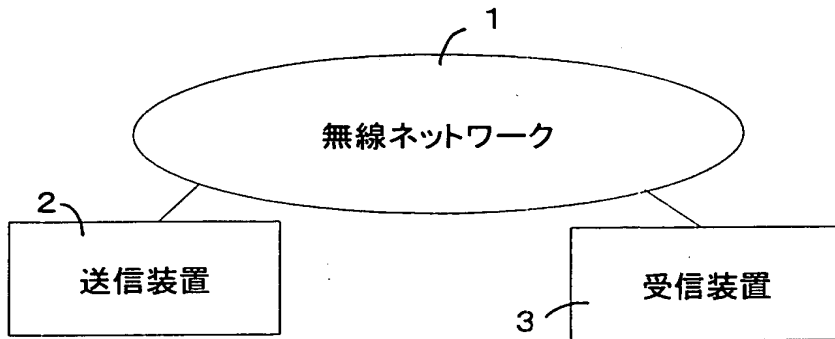
送信装置と受信装置が行うAVデータの暗号化伝送処理の第2の実施形態の処理手順を示すシーケンス図。

**【符号の説明】**

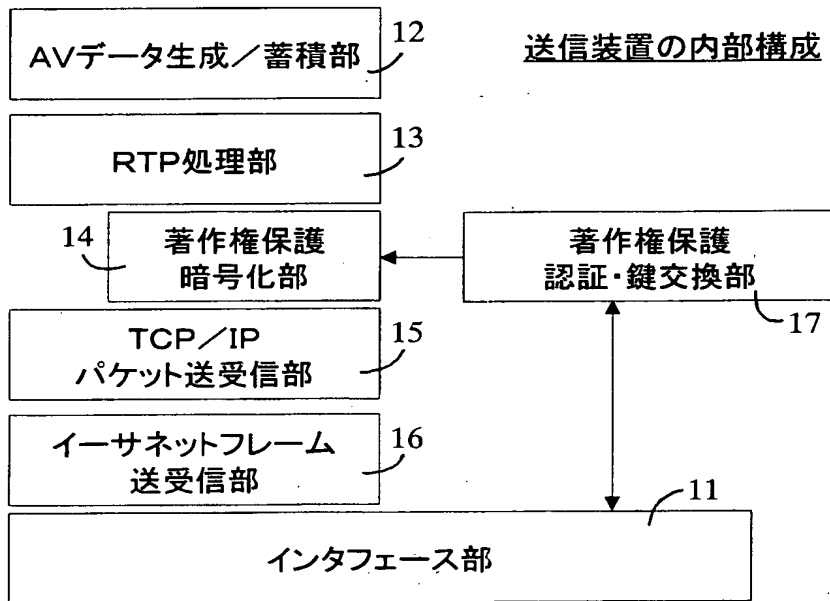
- 1 ホームネットワーク
- 2 送信装置
- 3 受信装置
- 1 1 インタフェース部
- 1 2 AVデータ生成／蓄積部
- 1 3 RTP処理部
- 1 4 著作権保護暗号化部
- 1 5 TCP/IPパケット送受信部
- 1 6 イーサネットフレーム送受信部
- 1 7 著作権保護認証・鍵交換部
- 2 1 インタフェース部
- 2 2 イーサネットフレーム送受信部
- 2 3 TCP/IPパケット送受信部
- 2 4 著作権保護復号化部
- 2 5 RTP処理部
- 2 6 AVデータ再生／蓄積部
- 2 7 著作権保護認証・鍵交換部

【書類名】 図面

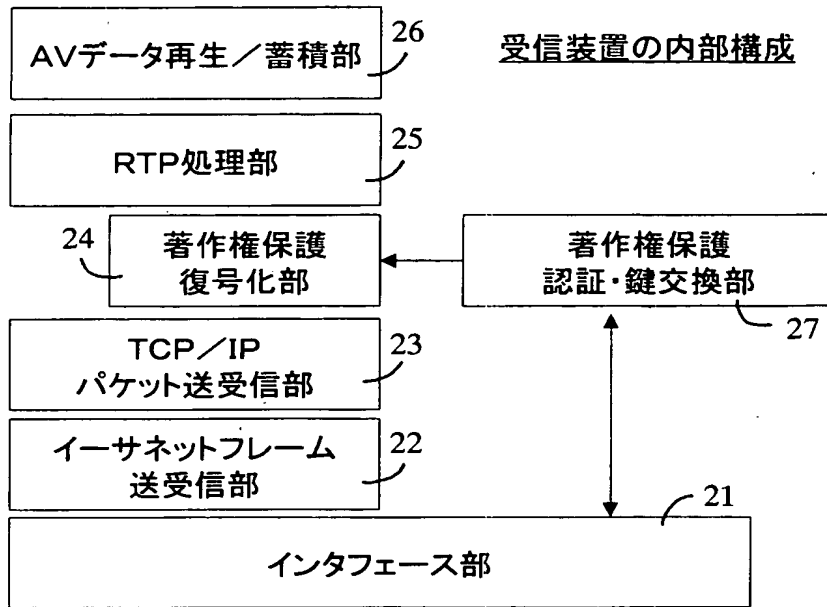
【図1】



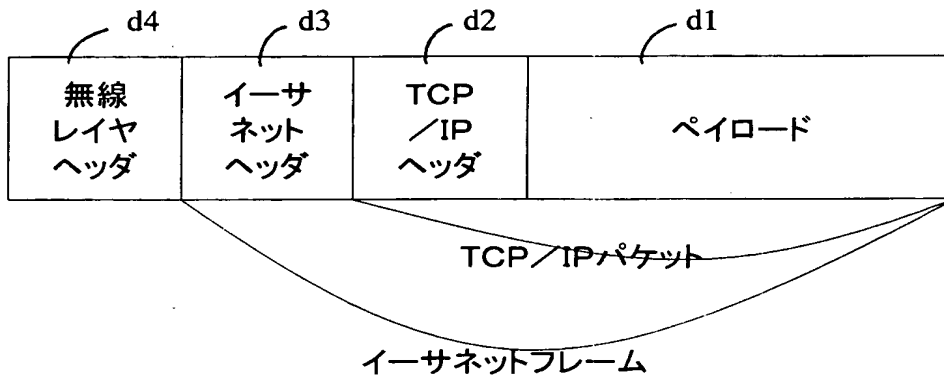
【図2】



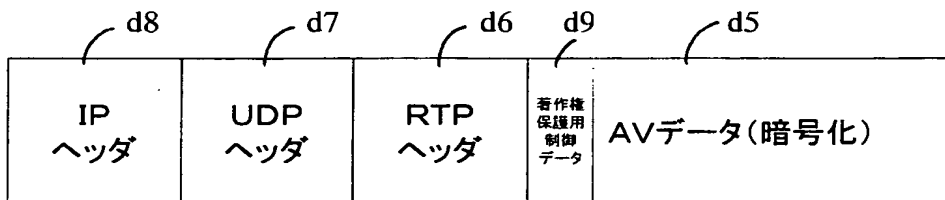
【図 3】



【図 4】



【図 5】









【書類名】 要約書

【要約】

【課題】 著作権保護を図りつつAVデータの送信または受信を行えるようにする

【解決手段】 AV通信システムは、ある家庭内のホームネットワーク1と、このホームネットワーク1に接続されている送信装置2及び受信装置3とを備えている。送信装置2及び受信装置3は、著作権保護を図る必要のあるAVデータを暗号化、または復号化し、著作権保護のために使用される特定のプロトコル(DTCTP)に関する情報と、ペイロードタイプの値を含むAV転送プロトコルヘッダ(RTPヘッダ)と、を付加したAVパケットの送信または受信を行うAVデータ処理手段と、著作権保護を施すAVデータを特定するための前記ペイロードタイプの値のネゴシエーションを、著作権保護のための認証・鍵交換処理の中で行う認証・鍵交換手段と、を備える。これにより、著作権保護を施すべきデータの識別が容易に行うことができるようになり、もって、著作権保護を図りつつ、AVデータを簡易かつ迅速に取得できる。

【選択図】 図1

特願2003-058927

出願人履歴情報

識別番号

[000003078]

1. 変更年月日 2001年 7月 2日  
[変更理由] 住所変更  
住 所 東京都港区芝浦一丁目1番1号  
氏 名 株式会社東芝
  
2. 変更年月日 2003年 5月 9日  
[変更理由] 名称変更  
住所変更  
住 所 東京都港区芝浦一丁目1番1号  
氏 名 株式会社東芝